

UNITED STATES DISTRICT COURT

for the
Western District of New York

August 24, 2015

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH E-MAIL ACCOUNT
Dariusouting123309@gmail.com STORED AT PREMISES CONTROLLED BY Google,
Inc.

Case No. 15-M- 108

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe property to be searched and give its location): See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 1014 & 1344, and the application is based on these facts: SEE AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

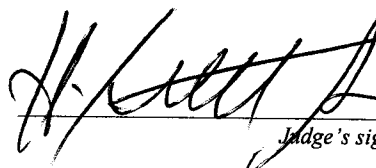
Marc Matla, SA, ICE HSI SAC

Printed name and title

Sworn to before me and signed in my presence.

Date: August 24, 2015

City and state: Buffalo, New York



Judge's signature

H. KENNETH SCHROEDER, JR., U.S. Magistrate Judge

Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the following Google Inc. e-mail account:

Darriusoutling123309@gmail.com

that is stored at premises owned, maintained, controlled, or operated by Google Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B
List of Items to be Seized

I. Information to be disclosed by Google Inc.

To the extent that the information described in **Attachment A** is within the possession, custody, or control of Google Inc., Google Inc. is required to disclose the following information to the government for the account or identifier listed in **Attachment A**:

- a. The contents of any and all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail.
- b. Any and all attachments to the e-mails described in (a) above.
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records or session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting log files, and means and source of payment (including any credit or bank account numbers).
- d. Any and all content and all records or other information stored by an individual using the account, including Friends lists, Photos, and Briefcase, in addition to any address books, contact and buddy lists, calendar data, pictures and files.
- e. Any and all Google IDs listed on the subscriber's Friends list.
- f. Any and all methods of payment provided by the subscriber to Google for any premium services.

II. Information to be seized by the government

- a. All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 United States Code

Sections 1014 (fraud concerning loan documents), 1343 (wire fraud) and 1344 (bank fraud), and Title 42 United States Code Section 408 (fraud regarding social security numbers).

b. All communications between e-mail addresses darriousoutling123309@gmail.com and terrym@raylaks.com, to include all attachments to said emails.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **Marc Matla**, being duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant to search the Google mail (or gmail) e-mail account darriusoutling123309@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google Inc. which is headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

2. The information to be searched is the evidence, fruits, or instrumentalities of violations of Title 18 United States Code Sections 1014 (fraud concerning loan documents), 1343 (wire fraud), 1344 (bank fraud), and Title 42 United States Code Section 408 (fraud regarding social security numbers), as further described in the following paragraphs and in **Attachments A and B**.

3. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

4. I am a Special Agent with United States (U.S.) Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed for approximately 5 years. I was previously employed with the United States Postal Inspection Service, the United States Secret Service, and the Virginia State Police. I am currently assigned to the Special Agent in Charge, Buffalo, New York office to investigate financial crimes within the Western District of New York. As part of my official duties, I investigate allegations of violations of federal criminal law, including statutes that prohibit fraud.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DETAILS OF THE INVESTIGATION

6. In December 2011, I received information that federally insured financial institutions, including Cornerstone Community Federal Credit Union (CCFCU), and State Employees Federal Credit Union (SEFCU) had received indirect loan applications from Terry McCormick, who is employed as a salesperson and finance specialist for Ray Laks Resale, 120 Orchard Park Rd., West Seneca, NY. The loan applications appeared to contain false information and forged documents, including fake Social Security Cards that contained false information.

7. On May 21, 2013, a Search and Seizure Warrant, issued by The United States District Court for the Western District of New York, was executed at Ray Laks Resale. Several items were seized, including a computer tower (CPU), SN 34504, located in an office identified by an employee at Ray Laks Resale as Terry McCormick's office. The computer was examined by an HSI computer forensics agent.

8. On July 19, 2013, I received the results from the computer forensics examination on that same CPU. Under the bookmark labeled "Outling", there were several images of Social Security Cards with different numbers imprinted on them. These images were emailed from email address darriusoutling123309@gmail.com to terrym@raylaks.com. I observed on the Ray Laks website that McCormick's email address is listed as terrym@raylaks.com.

9. One SSN card image had the name Artice McDowell and XXX-XX-0901 on it. This is the same image that was forwarded to Cornerstone Community Federal Credit Union (CCFCU), a federally insured financial institution, in attempt to secure a loan for McDowell through CCFCU. McDowell confirmed with your Affiant that this is not a copy of his SSN card nor is the number imprinted on it his SSN.

10. Another SSN card image was found to have the name Shinetta Hairston and XXX-XX-2275 on it. This is the same image that was forwarded to CCFCU in attempt to secure a loan for Hairston. Hairston confirmed with me that this is not a copy of her SSN card nor is the number imprinted on it her SSN.

11. Another SSN card image was found to have the name Latora Atcherson and XXX-XX-4129 on it. This is the same image that was forwarded to State Employees Federal Credit Union (SEFCU), a federally insured financial institution, in attempt to secure a loan for Atcherson. Atcherson confirmed with me that this is not a copy of her SSN card nor is the number imprinted on it her SSN.

12. Another SSN card image was found to have the name Thomas Medley and XXX-XX-7184 on it. This is the same image that was forwarded to SEFCU in attempt to secure a loan for Medley. Medley confirmed with me that this is not a copy of his SSN card nor is the number imprinted on it his SSN.

13. Another SSN card image was found to have the name Aaron Douglas and XXX-XX-2875 on it. This is the same image that was forwarded to SEFCU in attempt to secure a loan for Douglas. Douglas confirmed with me that this is not a copy of his SSN card nor is the number imprinted on it his SSN.

14. I confirmed with Special Agent Joan Torres, Social Security Administration, Office of the Inspector General (SSAOIG), that none of the aforementioned names and SSN's are assigned to those subjects.

15. On June 9, 2015, I met with Darrius Outling at the U.S. Attorney's Office for the Western District of New York pursuant to a proffer agreement.

16. Outling verified that his email address is darriusoutling123309@gmail.com. I showed Outling images of the aforementioned SSN cards that were contained in Outling's emails to McCormick. Outling stated that he imposed the names and numbers on the SSN card images and forwarded them to McCormick. Outling said that McCormick requested that Outling email the cards to him that way. Outling said that prior to his imposing names and numbers on the SSN cards, McCormick had supplied him with the template of a blank SSN card via email. Outling stated that this email containing the blank SSN card template came from McCormick to Outling's email address of darriusoutling123309@gmail.com.

17. I asked Outling to explain the nine digit numbers contained on the SSN cards from the emails, because they appear to be SSNs that he forwarded to McCormick through email. Outling explained that the numbers which appear to be SSNs are CPNs (Credit Profile Numbers). Outling said CPNs are used instead of SSNs by people who have bad credit. Outling said that McCormick had requested that Outling obtain CPNs for McCormick's customers. Outling said he purchased the CPNs over the internet. Outling said the use of a CPN is an alternative to a SSN so that people can build their credit.

18. Outling said he has not used his aforementioned email address in some time and does not remember the password to it. Outling also stated the he never deleted any emails that he received using that email address, including the email he described that he received from McCormick containing the blank template SSN card in it.

TECHNICAL BACKGROUND

19. In my training and experience, I have learned that Google Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google Inc. allows subscribers to obtain e-mail accounts at the domain name "gmail.com," like the e-mail account listed in **Attachment A**. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc., asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, e-mail transaction information, and account application information.

20. In general, an e-mail that is sent to Google Inc. subscribers is stored in the subscriber's "mail box" on Google Inc. servers respectively until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on the server indefinitely.

21. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google Inc. servers, and then transmitted to its end destination. Google Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google Inc. server, the e-mail can remain on the system indefinitely.

22. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google Inc. but may not include all of these categories of data.

23. Google Inc. can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google Inc.

24. Subscribers to Google Inc. might not store on their home computers copies of the e-mails stored in their internet based accounts. This is particularly true when they access their account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

25. In general, e-mail providers like Google Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

26. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and

durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google Inc.) and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

27. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

28. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I submit that probable cause exists to conduct a search of the Google e-mail account darriusoutling123309@gmail.com for evidence relating to violations of Title 18, United

States Code, Sections 1014 (fraud concerning loan documents), 1343 (wire fraud), 1344 (bank fraud), and Title 42, United States Code, Section 408 (fraud regarding social security numbers). It is anticipated that upon receipt of an executed search warrant, Google will provide an electronic copy of all e-mails, attachments, histories, subscriber information, method of payment, and log on and off times for the e-mail account in question. Upon receipt of this information, myself and other Special Agents will search all of the items provided for evidence related to violations of Title 18, United States Code, Sections 1014, 1343 and 1344, and Title 42, United States Code, Section 408.

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of **Attachment B**, which is attached hereto and incorporated as if fully set forth herein. Upon receipt of the information described in Section I of **Attachment B**, government-authorized persons will review that information to locate the items described in Section II of **Attachment B**, which is attached hereto and incorporated as if fully set forth herein.

CONCLUSION


31. Based on the forgoing, I believe that there is probable cause of violations of Title 18, United States Code, Sections 1014 (fraud concerning loan documents), 1343 (wire fraud), 1344 (bank fraud), and Title 42, United States Code, Section 408 (fraud regarding social security numbers). Additionally, there is probable cause to believe that evidence concerning these

violations exists on mail servicers of Google and within the Google e-mail account darriusoutling123309@gmail.com as described in **Attachment A**.

32. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 42 U.S.C. § 408(a)(7).


33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

34. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the property known as the email servers of Google and within the Google email account darriusoutling123309@gmail.com, which is more fully described in **Attachment A**, authorizing the search of the aforementioned property for the items described in **Attachment B**.



Marc Matla
Special Agent
ICE HSI SAC/Buffalo

Subscribed and sworn to before me
this 24th day of August, 2015.



HONORABLE H. KENNETH SCHROEDER JR.
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the following Google Inc. e-mail account:

Darriusoutling123309@gmail.com

that is stored at premises owned, maintained, controlled, or operated by Google Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B
List of Items to be Seized

I. Information to be disclosed by Google Inc.

To the extent that the information described in **Attachment A** is within the possession, custody, or control of Google Inc., Google Inc. is required to disclose the following information to the government for the account or identifier listed in **Attachment A**:

- a. The contents of any and all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail.
- b. Any and all attachments to the e-mails described in (a) above.
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records or session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting log files, and means and source of payment (including any credit or bank account numbers).
- d. Any and all content and all records or other information stored by an individual using the account, including Friends lists, Photos, and Briefcase, in addition to any address books, contact and buddy lists, calendar data, pictures and files.
- e. Any and all Google IDs listed on the subscriber's Friends list.
- f. Any and all methods of payment provided by the subscriber to Google for any premium services.

II. Information to be seized by the government

- a. All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 United States Code

Sections 1014 (fraud concerning loan documents), 1343 (wire fraud) and 1344 (bank fraud), and Title 42 United States Code Section 408 (fraud regarding social security numbers).

b. All communications between e-mail addresses darriiousoutling123309@gmail.com and terrym@raylaks.com, to include all attachments to said emails.